Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1110

Vragen van het lid **Klein** (Klein) aan de Minister van Sociale Zaken en Werkgelegenheid over *het bericht van Techzine van 2 december* (ingezonden 4 december 2015).

Antwoord van Minister **Asscher** (Sociale Zaken en Werkgelegenheid), mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 14 januari 2016).

Vraag 1
Kent u het bericht van Techzine van 2 december 2015 «UWV lekt mogelijk persoonsgegevens via MijnUWV»?[1] [2]

Antwoord 1
Ja.

Vraag 2
Hoe kan het dat mensen na inloggen in MijnUWV de gegevens van een ander te zien krijgen?

Antwoord 2
UWV heeft geen meldingen van klanten ontvangen dat de gegevens van een ander te zien zijn na inloggen op MijnUWV. Wel is er een beperkt aantal incidenten bekend waarbij klanten de gegevens van een ander inzagen bij het inloggen op werk.nl. UWV heeft hier 20 meldingen van ontvangen. Inmiddels zijn er maatregelen getroffen waardoor deze incidenten zich niet meer voordoen.
De incidenten bij het inloggen op werk.nl werden veroorzaakt door een software-fout in de firewall van de internetprovider van UWV. Hierbij werd de pagina van een klant abusievelijk deels gevuld met gegevens van een ander. De klant kon dan personalia, contactgegevens en in sommige gevallen het beroep van een andere klant zien. Deze gegevens verdwenen met elke volgende klik op de webpagina. Nader inzien van gegevens was dan ook niet mogelijk. Financiële gegevens konden niet worden ingezien.

[1] http://m.techzine.nl/nieuws/42420/uwv-lekt-mogelijk-persoonsgegevens-via-mijnuwv.html
[2] UWV: Uitvoeringsorganisatie Werknemersverzekeringen

ah-tk-20152016-1110
ISSN 0921 - 7398
’s-Gravenhage 2016

Vraag 3
Heeft dit te maken met de storing die deze week plaats vond, of betreft dit een fundamenteel probleem?

Antwoord 3
Nee, er is geen enkele relatie met de tijdelijke storing van MijnUWV. Ook betreft dit geen fundamenteel probleem. Inmiddels zijn er maatregelen getroffen waardoor de incidenten op werk.nl zich niet meer voordoen.

Vraag 4
Van hoeveel mensen zijn de gegevens op straat komen te liggen?

Antwoord 4
Er zijn geen klantgegevens op straat komen te liggen. Wanneer het incident zich voordeed, waren na een klik de gegevens direct verdwenen (zie antwoord[3].
UWV heeft in totaal 20 meldingen van klanten ontvangen dat zij gegevens van anderen konden inzien bij het inloggen op werk.nl. Gezien op het totaal van 100.000 ingelogde werkzoekenden per dag is dit een zeer klein aantal, echter vindt UWV elk incident er één teveel. Inmiddels zijn er maatregelen getroffen waardoor deze incidenten zich niet meer voordoen.

Vraag 5
Welke acties worden ondernomen om het lekken van gegevens in de toekomst te voorkomen?

Antwoord 5
UWV heeft meteen na de eerste melding actie ondernomen, heeft contact opgenomen met de melder en heeft in samenwerking met de leveranciers het onderzoek gestart naar de oorzaak van het probleem. Op basis van de eerste resultaten van het onderzoek heeft KPN maatregelen getroffen. Zo heeft KPN tijdelijk een vervangende firewall ingezet waardoor het probleem zich niet meer voordoet.
UWV en KPN werken samen aan het herstel van de oorspronkelijke firewall. De hiervoor benodigde software-update is opgeleverd en wordt momenteel uitvoerig getest voordat overgegaan wordt tot implementatie.

Vraag 6
Hoe worden mensen geïnformeerd over dit manco en wat doet u om eventuele schade die hieruit voortvloeit voor mensen te compenseren?

Antwoord 6
Met de klant die de melding deed is telefonisch overleg geweest. UWV heeft daarmee specifiekere informatie gekregen en heeft de klanten nadere uitleg kunnen verschaffen. De klant die daar prijs op stelden zijn telefonisch geïnformeerd over de voortgang van de oplossing. Voor zover bekend hebben klanten geen schade opgelopen en is er geen aanleiding mensen te compenseren.

Vraag 7
In hoeverre heeft u met MijnUWV rekening gehouden met de richtsnoeren van het College Bescherming Persoonsgegevens (CBP), inzake de beveiliging van persoonsgegevens?

Antwoord 7
UWV houdt rekening met de richtsnoeren van het CBP. Binnen de rijksoverheid worden het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijksdienst (BIR) toegepast. Aan UWV en de andere zelfstandige bestuursorganen (zbo's) is gevraagd dit normenkader te adopteren als richtlijn voor maatregelen op de informatie-beveiliging. De VIR en de BIR zijn beide gebaseerd op de standaard ISO 27001-code informatiebeveiliging. UWV heeft zijn tactische beleidskader voor beveiliging en privacy grotendeels op deze code gebaseerd. In mei 2014 heeft UWV met de

[3] UWV: Uitvoeringsinstelling Werknemersverzekeringen

ondertekening van de Bestuurlijke verklaring Informatieveiligheid zbo's de toepassing van de VIR/BIR bekrachtigd. In de nieuwe systematiek meet UWV continu of UWV blijvend voldoet aan de BIR standaard. Dit doet UWV onder andere via businessimpactanalyses en privacyimpact-analyses.